2008-09

Detection of IED emplacement in urban environments

O'Hara, Matthew

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DETECTION OF IED EMPLACEMENT IN URBAN ENVIRONMENTS

by

Matthew O'Hara

September 2008

Thesis Advisor: Gurminder Singh
Second Reader: Arijit Das

Approved for public release, unlimited distribution

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2008	**3. REPORT TYPE AND DATES COVERED** Dissertation	
4. TITLE AND SUBTITLE: Detection of IED Emplacement in Urban Environments		**5. FUNDING NUMBERS**	
6. AUTHOR(S): Matthew O'Hara, Lieutenant, United States Navy			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, unlimited distribution		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

This research will be focused on discovering patterns of activity that lead to the emplacement of IEDs by terrorists in urban environments. This research will employ a network in a predictive mode by looking for suspicious activity patterns and raising alerts when a pre-determined level of confidence is achieved in the prediction.

The scope of this thesis will be to conduct various experiments using wireless sensor network motes to detect the presence of magnetic material. Using various configurations of the motes, a pattern will be established that best predicts the presence of IEDs in a busy urban environment. The configurations will be designed and tested for reliability and coverage to support detection in various urban settings.

The results show that wireless sensor networks in conjunction with other anti-IED methods prove useful for the detection of IED material in urban settings. A wireless sensor network configured with proper equipment provides useful results for detecting IEDs and shows potential for correctly predicting behavior associated personnel carrying IED material.

14. SUBJECT TERMS IED, WSN, mote, magnetic			**15. NUMBER OF PAGES** 61
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DETECTION OF IED EMPLACEMENT IN URBAN ENVIRONMENTS

Matthew P. H. O'Hara
Lieutenant, United States Navy
B.S. Aeronautical Engineering, United States Navy Academy, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTERS OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2008

Author: Matthew P. H. O'Hara

Approved by: Gurminder Singh
Thesis Advisor

Arijit Das
Second Reader

Peter J. Denning,
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research will be focused on discovering patterns of activity that lead to the emplacement of IEDs by terrorists in urban environments. This research will employ a network in a predictive mode by looking for suspicious activity patterns and raising alerts when a pre-determined level of confidence is achieved in the prediction.

The scope of this thesis will be to conduct various experiments using wireless sensor network motes to detect the presence of magnetic material. Using various configurations of the motes, a pattern will be established that best predicts the presence of IEDs in a busy urban environment. The configurations will be designed and tested for reliability and coverage to support detection in various urban settings.

The results show that wireless sensor networks in conjunction with other anti-IED methods prove useful for the detection of IED material in urban settings. A wireless sensor network configured with proper equipment provides useful results for detecting IEDs and shows potential for correctly predicting behavior associated personnel carrying IED material.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I personally want to thank the members of the Armed Forces bravely serving our country in the war on terrorism. The sacrifices of the many brave individuals serving will never be forgotten.

In regards to this thesis, I would like to thank Arijit Das for his countless hours of support in setting up the experiments and providing many useful suggestions for the experiments. I also want to thank Dr. Gurminder Singh for being my thesis advisor and patiently providing guidance for the work.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. IMPROVISED EXPLOSIVE DEVICE (IED) THREATS

An Improvised Explosive Device (IED) is defined as "a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract."[1] These rudimentary bombs generally consist of commonly found, non-military materials.

Improvised Explosive Devices have existed since the Chicago Haymarket Riot in 1886. However, IEDs currently provide the largest obstacle to coalition forces fighting in the Middle East. Terrorists construct these small devices and inflict grave damage upon military equipment and personnel. American casualties are not immune to the effects of IEDs. IED attacks account for over 60% of Operation Iraqi Freedom (OIF) casualties and 50% of Operation Enduring Freedom (OEF) casualties.[2] The first reported IED attack on American forces in Iraq occurred on March 29, 2003.[3] Since that first Iraqi attack, there have been over 81,000 IED attacks and over 25,000 in IED attacks in 2007 alone.[4]

1 "Counter-IED Technology." JIEDDO webpage. <https://www.jieddo.dod.mil/CIEDTECHNOLOGY/CIEDTECHHOME.ASPX>.

2 Wilson, Clay. "Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures." CRS Report for Congress 28 July 2007. p. 1.

3 Atkinson, Rick. "The single most effective weapon against our deployed forces" The Washington Post 30 September 2007. <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/29/AR2007092900750.html>.

4 Ibid.

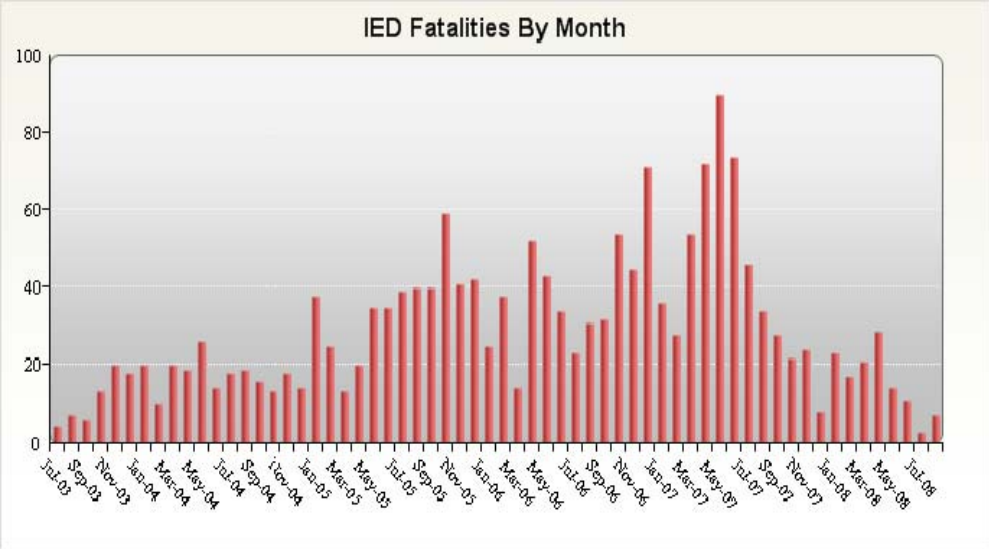

Figure 1. Coalition Forces IED Fatalities (From icasualties.org, September 2008)

Insurgent cells constructing IEDs are small, highly trained groups that remain as hidden as possible. The IED groups consist of six to eight people, including a financier, bomb maker, emplacer, triggerman, spotter, and cameraman.[5] Despite US-led efforts to find these cells, new cells repeatedly form in Iraq. Estimates include 160 bomb-making cells in Iraq.

Although common IED threats include roadside bombs, suicide bombers are another emerging problem in the IED arena. Suicide bombers carrying Personal-borne IEDs (PBIEDs) are extremely hard to detect or stop. Because no IED emplacement is necessary, a suicide bomber can quickly strap on an IED-laden vest and move to the kill zone. Placed in the proper urban environment, this weapon is capable of inflicting serious structural damage and killing hundreds of people in mere seconds.

B. AMERICAN RESPONSE

As America attempts to counter the IED problem, bomb makers continually improve their construction techniques. Each new IED is increasingly more advanced and

5 Wilson, Clay. "Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures." CRS Report for Congress 28 July 2007. p. 2.

sophisticated then its previous version. Each time an effective solution is found, bomb-making cells react with a counterstrike solution. The constant game of cat and mouse has proved difficult for American forces fighting in Iraq and Afghanistan.

The six principal detonation triggers are pressure plates, cell phones, command wire, low-power radio-controlled, high-powered radio-controlled, and passive infrared.[6] At first, most IEDs employed the cell phone and radio triggers. America responded by rapidly deploying electronic countermeasures or "jamming" techniques. Employing jammers in the field effectively reduced the radio-controlled IEDs to less than 10 percent of the IEDs. The terrorists responded by employing the simpler pressure plate and command wire models. However, the bomb makers developed the more advanced passive infrared trigger. These triggers were immune to most American electronic countermeasures techniques employed to stop cell phone and radio-controlled attacks. The small lens used for the passive infrared detector was extremely difficult to see or locate.[7]

The US also provided heavier armor for its convoy vehicles. Once again, the bomb makers found a counter-solution. Newer IED designs include explosively formed projectiles (EFPs) that penetrate vehicle armor.

In addition to IED cell ingenuity, nation-states like Iran reportedly support the insurgencies by funding IED technology advancement. State-sponsored funding exponentially increases the effectiveness of new IEDs and is the source of EFP material used against coalition forces.

The need for effective IED countermeasures led the America to form the Army IED Task Force in October 2003, which was later transformed into the Joint IED Task Force. The Joint IED Task Force was officially deemed the Joint IED Defeat Organization (JIEDDO) in February 2006 under Department of Defense (DOD) Directive

---

6 Wilson, Clay. "Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures." CRS Report for Congress 28 July 2007. p. 2.

7 Atkinson, Rick. "If you don't go after the network, you're never going to stop these guys. Never." The Washington Post 3 October 2007. <http://www.washingtonpost.com/wp-dyn/content/article/2007/10/02/AR2007100202366.html>.

2000.19E. The purpose of JIEDDO is to mitigate the IED problem by attacking the threat, increasing IED research, and training the DOD in IED matters. JIEDDO is split among three Lines of Operation including: 1) attack the network, 2) defeat the device and, 3) train the force. The organization has spent $375 million countering the IED problem since 2003.[8]

C. THESIS SCOPE

The work in this thesis concentrates on detection of magnetic materials used in IEDs in urban environments using a wireless sensor network. Using the magnetic detectors in the wireless sensor nodes, magnetic behaviors and patterns are analyzed to differentiate a person carrying an IED and a person possessing magnetic material like jewelry or key chains. Using wireless sensor nodes instead of standard metal detectors enables the detectors to remain hidden to outside observers. The small nodes easily blend into the indigenous environmental settings to provide stealth.

Differing wireless sensor network configurations were tested and analyzed to discover an optimal wireless sensor network topology solution for detecting patterns of IED behavior consistent with that of personal-borne IEDs (PBIEDs). Specifically, the thesis work analyzed magnetic detection of IED material through a building entrance or doorway in a busy urban setting. The thesis experimentation and conclusions determined the feasibility of using wireless sensor networks for IED detection and countermeasures in an urban environment.

D. THESIS ORGANIZATION

This thesis is broken into five chapters. The first chapter introduces the growing IED problem American troops face in Iraq. The second chapter analyzes the components and structure of an IED and shows various countermeasures the United States has undergone to lessen the effects of IEDs. Chapter III gives a basic introduction to wireless sensor networks and its applicability in solving various problems. Chapter IV reviews

[8] Chisolm, Patrick. "Clearing the Roads." *Special Operations Technology Online Edition.* 2 July 2008. <http://www.special-operations-technology.com/article.cfm?DocID=1129>.

the work and experiments conducted for solving magnetic detection of IED behavior in urban settings. Chapter V presents the conclusions of the thesis experiments and proposes suggestions for future work in strengthening the use of wireless sensor networks for IED countermeasures.

THIS PAGE INTENTIONALLY LEFT BLANK

II. IED COUNTERMEASURES

A. IED COMPONENTS

Every bomb maker has a unique signature for each IED created. However, there are five common components in IEDs that are necessary to inflict maximal damage with minimal assembly.

1. Power Source

All IEDs require a power source to initiate the weapon. Most initiators are battery operated electrical devices, but there are other means of initiation. Spring-loaded initiators require no electrical power source to function.[9]

Figure 2. IED power source (From longwarjournal.org, September 2008)

[9] "Explosive Devices." Department of Homeland Security, Office of Domestic Preparedness 9 June 2005. p. 88.

2. Initiator/Detonator

The IED initiator detonates the weapon and begins the bombing sequence. Common initiators are blasting caps and fuse igniters. Electrical initiators can be triggered in various ways, including a button, radio frequency, optical, etc.[10]

Figure 3. IED blasting cap (From stresau.com, September 2008)

3. Explosives

Common explosive materials are TNT, potassium chlorate, triacetonetriperoxide, ammonium nitrate and aluminum powder, and urea nitrate. These chemicals produce the explosive effect of the IED.[11]

4. Switch

The IED switch arms the weapon after the initiator sequence begins. The switch could be an arming switch, fuse, or both for redundancy. Once the IED is armed, the internal circuit is complete and detonation occurs shortly thereafter.[12]

---

10 "Explosive Devices." Department of Homeland Security, Office of Domestic Preparedness 9 June 2005. p. 89.

11 Ibid., p. 89.

12 Ibid., p. 89.

Figure 4. IED pressure switch (From eastarmy.nic.in, September 2008)

5. Fragmentation and Shrapnel

The explosive material in an IED is quite deadly, but the damaging effect is maximized by adding fragmentation and shrapnel to the weapon. Standard materials are steel ball bearings, nails, staples, etc.[13]

B. IED EXPLOSIVE MATERIALS

1. Potassium Chlorate

Potassium Chlorate is commonly found in fireworks and is easily obtainable. The explosive looks like white crystals or powder and has 83% of TNT power.[14]

2. Triacetonetriperoxide

Triacetonetriperoxide (TATP) is the most common explosive used by Middle Eastern suicide bombers. TATP consists of peroxide, sulfuric acid, and acetone. The combination yields 88% of TNT explosive power. TATP appears as a white powder similar to cocaine.[15]

---

13 "Explosive Devices." Department of Homeland Security, Office of Domestic Preparedness 9 June 2005. p. 89.

14 Ibid., p. 86.

15 Ibid., p. 87.

3. Ammonium nitrate and Aluminum Powder

Both ammonium nitrate powder and aluminum powder are common hardware store materials that combine to yield a 75% explosive effect to that of TNT. Ammonium nitrate is commonly found in fertilizer, while aluminum powder is simply aluminum metal ground into a powder.[16]

4. Urea Nitrate

Urea nitrate consists of nitric acid and urea. Nitric acid is one of the most commonly produced chemicals worldwide and can be found in most fertilizers. Urea is also easily obtainable from many forms, including concentrated urine. This combination yields a 75% TNT explosive effect.[17]

C. IED TYPES

1. Packaged IED

Packaged IEDs are the standard homemade bomb used by Iraqi insurgents. Although variable in size, they are generally small enough to be carried by one person. These types of IEDs can be buried underground, placed in trashcans, or even thrown at their intended target. Packaged IEDs usually contain military munitions as its explosive component.[18]

16 "Explosive Devices." Department of Homeland Security, Office of Domestic Preparedness 9 June 2005. p. 87.

17 Ibid., p. 88.

18 "Package-Type Improvised Explosive Devices (IEDs)." GlobalSecurity.org 11 January 2005. <http://www.globalsecurity.org/military/intro/ied-packaged.htm>.

Figure 5. Packaged IED in concrete casing (From GlobalSecurity.org, September 2008)

2. Vehicular-borne IEDs (VBIEDs)

Vehicular-borne IEDS (VBIEDs) are bombs constructed with a vehicle as the delivery device. Much larger than the packaged IEDs, VBIEDS contain more explosive material and are more lethal than typical IEDs.[19]

19 "Vehicle Borne IEDs (VBIEDs)." GlobalSecurity.org 11 January 2005. <http://www.globalsecurity.org/military/intro/ied-vehicle.htm>.

BATF Explosive Standards

ATF	Vehicle Description	Maximum Explosives Capacity	Lethal Air Blast Range	Minimum Evacuation Distance	Falling Glass Hazard
	Compact Sedan	500 pounds 227 Kilos (In Trunk)	100 Feet 30 Meters	1,500 Feet 457 Meters	1,250 Feet 381 Meters
	Full Size Sedan	1,000 Pounds 455 Kilos (In Trunk)	125 Feet 38 Meters	1,750 Feet 534 Meters	1,750 Feet 534 Meters
	Passenger Van or Cargo Van	4,000 Pounds 1,818 Kilos	200 Feet 61 Meters	2,750 Feet 838 Meters	2,750 Feet 838 Meters
	Small Box Van (14 Ft. box)	10,000 Pounds 4,545 Kilos	300 Feet 91 Meters	3,750 Feet 1,143 Meters	3,750 Feet 1,143 Meters
	Box Van or Water/Fuel Truck	30,000 Pounds 13,636 Kilos	450 Feet 137 Meters	6,500 Feet 1,982 Meters	6,500 Feet 1,982 Meters
	Semi-Trailer	60,000 Pounds 27,273 Kilos	600 Feet 183 Meters	7,000 Feet 2,134 Meters	7,000 Feet 2,134 Meters

Table 1. VBIED Explosive effect (From GlobalSecurity.org, September 2008)

3. Personal-borne IEDs (PBIEDs)

The personal-borne IED (PBIED) is the suicide bomber with explosives strapped to the body. The PBIED is often well concealed on the body and difficult to detect without personal inspection. Suicide bombers are highly mobile and inflict maximal damage in crowded urban areas. Since the suicide bomber dies upon PBIED detonation, this type of enemy is extremely difficult to combat.

Figure 6. Actual PBIED vest used by Sri Lankan terrorist (From Asian Tribune, September 2008)

D. METHODS OF DETECTION

There are many methods currently being employed in the hunt for IEDs in Iraq. JIEDDO has increasingly stepped up its efforts in combating the problem, but the issue still plagues American troops. Bomb makers consistently deliver bomb solutions that thwart American anti-IED efforts.

1. Electromagnetic Energy

One of the first American solutions was to detect the frequency spectrum used by the IED initiator devices. By correctly analyzing the frequency spectrum used by the remote triggers, troops successfully jammed the frequencies and prevented IEDs from being triggered. Electromagnetic pulse jamming also destroyed IED circuitry. Warlock Blue is a small, portable jamming device carried by troops into the battlefield. Produced by Tyco, the device specifically targets the IED triggering mechanisms.[20]

[20] Mortenson, Darrin. "Electronic 'IED' jammers roll out to stymie bombers." *North County Times* 10 July 2005. <http://www.globalsecurity.org/org/news/2005/050710-ied-jammers.htm>.

2. Change Detection

Unmanned Aerial Vehicles (UAVs) use mounted cameras to take pictures of probable IED areas and then come back for more images. The Buckeye camera mounted on a UAV uses an electro-optical sensor capable of producing three-dimensional images. Using imagery software or the human eye, the Buckeye pictures are analyzed against pictures from the same area, but taken at a different time. Scrutinizing the images to the nearest pixel, experts can determine if suspicious IED activity has occurred in a region. The Army's Shadow UAV Detection System also employs cameras for change detection. Another system, the ULTOR (Ultra Lethal Targeting by Optical Recognition) high-speed optical processor recognizes IEDs and employs precision tracking for vehicles. The ULTOR system uses the Internet, allowing it to be used anywhere in the world.[21]

Many different tools and technologies analyze images for change detection. Image analysis is currently one of the most successful methods currently in use for countering insurgent IEDs. Research in change detection has extended to many battlefield applications and is another resource used for IED countermeasures.

Figure 7. ULTOR processor (From aos-inc.com, September 2008)

[21] Farr, Keith. "ULTOR: Ultra Lethal Targeting by Optical Recognition." Advanced Optical Systems, Inc. 2006. <http://www.aos-inc.com/research/TechBriefPDFs/ULTORTechBrief.pdf >.

3. Chemical

Many studies test the chemical properties of IED materials and the surrounding environment of IED emplacement. The BAE Talon Radiance II hyperspectral sensor system in conjunction with the Shadow UAV uses hyperspectral sensing to identify materials.[22] Hyperspectral sensing, or imaging spectroscopy, identifies materials and elements by measuring chemical bonds within the material.[23] Raman spectroscopy is another method used to detect IED material. Raman spectroscopy measures the wavelength and intensity of inelastic scattered light and provides molecular information about a material[24]. A study conducted by the New Mexico Institute of Mining and Technology from 2004-06 measured soil moisture content and other environmental soil properties to find buried IEDs[25]. Although the study was inconclusive for real world IED emplacement, it showed a promising area for further research.

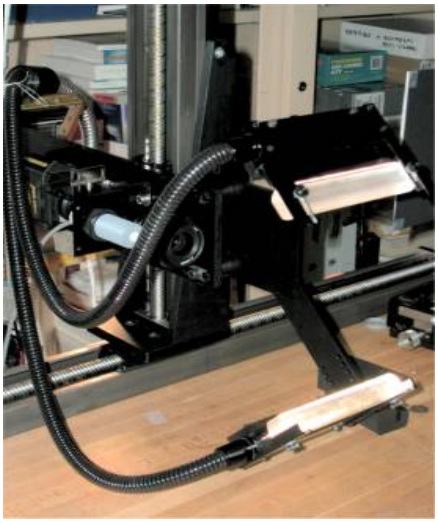

Figure 8. Hyperspectral Sensor (From ifac.cnr.it, September 2008)

---

[22] Chisolm, Patrick. "Clearing the Roads." *Special Operations Technology Online Edition.* 2 July 2008. <http://www.special-operations-technology.com/article.cfm?DocID=1129>.

23 Clark, Roger. "About Imaging Spectroscopy." US Geological Survey 25 September 2002. <http://speclab.cr.usgs.gov/aboutimsp.html>.

24 Tissue, Brian. "Raman Spectroscopy." Science Hypermedia Home Page 24 February 1996. <http://elchem.kaist.ac.kr/vt/chem-ed/spec/vib/raman.htm>.

25 Hendrickx et al. "New Mexico Tech Landmine, UXO, IED Detection Sensor Test Facility: Measurement in Real Field Soils." New Mexico Institute of Mining and Technology 27 April 2006. p. 1.

The Idaho National Laboratory developed the Idaho Explosives Detection System using pulsed thermal neutron generation. This method changes the molecular material structure to emit gamma rays. The gamma rays are then analyzed by sodium-ion detectors to identify nitrogen-based explosives. Nitrogen is found in over 98% of all explosives.[26] This exciting technology provides solutions to many military problems, especially IED issues.

Figure 9. Idaho Explosives Detection System in use (From inl.gov, September 2008)

4. Other Solutions

Many organizations are working on anti-IED technology in coordination with JIEDDO. All Optronics Inc. proposes to pre-treat areas with fluorescent material and then use optical imaging to detect and analyze changes within the treated areas.[27] The DOD Sensor Countermeasures for the Future Force program will investigate solutions involving airborne sensors, communications, and battlefield surveillance radar.[28]

---

[26] Huffman, Ethan. "INL's Explosive Detection System to be installed at US Air Base." Idaho National Laboratory 21 November 2006. <http://www.inl.gov/featurestories/2006-11-21.shtml>.

[27] Chisolm, Patrick. "Clearing the Roads." *Special Operations Technology Online Edition.* 2 July 2008. <http://www.special-operations-technology.com/article.cfm?DocID=1129>.

[28] Chisolm, Patrick. "Clearing the Roads." *Special Operations Technology Online Edition.* 2 July 2008. <http://www.special-operations-technology.com/article.cfm?DocID=1129>.

Magnetic sensors used to detect metallic IED materials are being developed for use in the battlefield. The National Institute of Standards and Technology (NIST) has developed a tiny magnetometer requiring very little power to operate.[29]

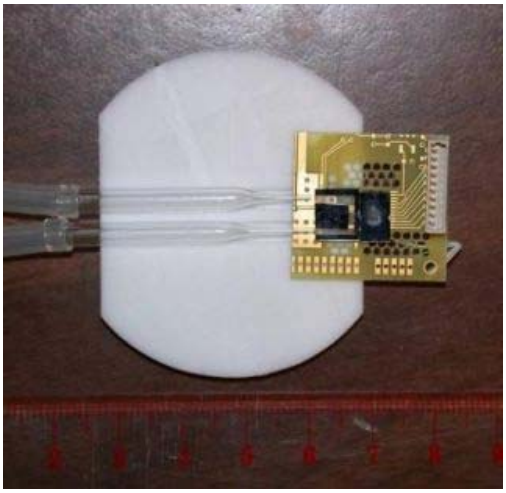

Figure 10. NIST Magnetometer (From physorg.com, September 2008)

Through a cooperative effort among the numerous government contractors, a wealth of IED solutions is being investigated. Research is being conducted in analyzing all aspects of an IED from its physical and chemical composition all the way to the bomb maker. As solutions arise, America must be able to attack counter-solutions of the bomb makers.

E. SUMMARY

There are countless numbers of IED countermeasures solutions currently being researched, developed, and analyzed by US contracting organizations and JIEDDO. Each solution must accurately react to past IED problems and predict future IED scenarios. Predicting future IED weapons and detonation methods is an exhaustive challenge that is nearly impossible to solve. As bomb makers continually develop solutions to American

29 Bourzac, Katherine. "Tiny, Sensitive Magnetic-Field Detectors: Arrays of cheap magnetic sensors could detect improvised explosive devices." Technology Review, Massachusetts Institute of Technology 16 November 2007. <http://www.technologyreview.com/Biotech/19724/>.

countermeasures, the challenge is to keep up. Simple reaction to past IED scenarios merely provides a temporary Band-Aid that does not fully address the IED problem. As different solutions are analyzed, each must have the larger scope picture in mind, yet still be detailed enough to solve its individual piece of the IED puzzle.

This thesis uses wireless sensor network technology to counter personal-borne IEDs in urban environments. The next chapter provides a brief description of wireless sensor networking, its uses, and its applicability to an IED solution.

III. WIRELESS SENSOR NETWORKS FOR IED DETECTION

A. OVERVIEW

1. Background

A wireless sensor network (WSN) is formed from a series of wireless network nodes or motes, generally in an ad-hoc network configuration. Each node contains a small processor to handle sensing duties. Nodes are able to relay information using a pre-determined routing protocol such as ZigBee. The ZigBee protocol follows the IEEE 802.15.4 standard for wireless personal area networks employing low data rates and low power requirements. Due to the wireless constraint, each WSN node needs a self-contained power source such as batteries. Batteries make each mote power-limited and unable to sustain continuous long-term operations. Due to small power availability, nodes are constrained in processing and signaling capability. Many nodes have a "sleep" capability that allow the nodes to shut down their internal processors when not in use and increase battery life. Wireless sensor nodes possess sensing capabilities such as magnetic, passive infrared, acoustic, or etc. A series of cooperative wireless nodes with sensing capabilities results in a wireless sensor network.

A standard WSN uses the nodes for their physical sensing capabilities in conjunction with a special node called a base station. Although it is possible for the base station to be a node within the network, this is an unlikely situation. The base station receives information from the nodes and passes it to another source to process the data. Since the base station receives input from the WSN nodes, it has higher power requirements and must always coordinate data delivery out of the network.

2. Applications

Wireless sensor networks posses many useful real-world applications. Examples that WSN uses include:

- Environmental monitoring
- Industrial sensing and diagnostics
- Infrastructure protection
- Battlefield awareness
- Context-aware computing[30]

Wireless sensor network applications cover a broad spectrum from civilian to military use. Pickberry Vineyards in Sonoma County, CA employs a WSN measuring temperature, humidity, and soil moisture.31 Using the WSN allows the vineyard to accurately predict grape growth and properly apply changes necessary in producing premium wine. Researchers from the University of California, Berkeley setup a WSN on Great Duck Island, Maine to study the environment of the Leach's Storm Petrel bird.32 The practical applications of wireless sensor are endless, while WSN usage increasingly becomes commonplace even in the most unexpected places.

3. Basic Setup

A standard wireless sensor network configuration involves several wireless nodes and a base station. Each node contains sensing capabilities appropriate for the network application and needs. Nodes cannot process or analyze the information, but can forward information to either another node or the base station. The base station can be a specially designated node in the network or a completely separate entity. The base station then transmits received information to a network, computer, or transceiver capable of analyzing and processing information received from the WSN.

30 Zhao, Feng and Guibas, Leonidas. Wireless Sensor Network: An Information Processing Approach. Morgan Kaufmann Publishers, San Francisco, CA 2004. pp. 9-10.

31 Collins, Michael. "Wireless Sensor Network Helps Grower Produce Better Grapes." BBC News Online 6 July 2004. <http://news.bbc.co.uk/2/hi/technology/3860863.stm>.

32 Mainwaring et al. "Wireless Sensor Networks for Habitat Monitoring." WSNA '02, Atlanta, GA 28 September 2002.

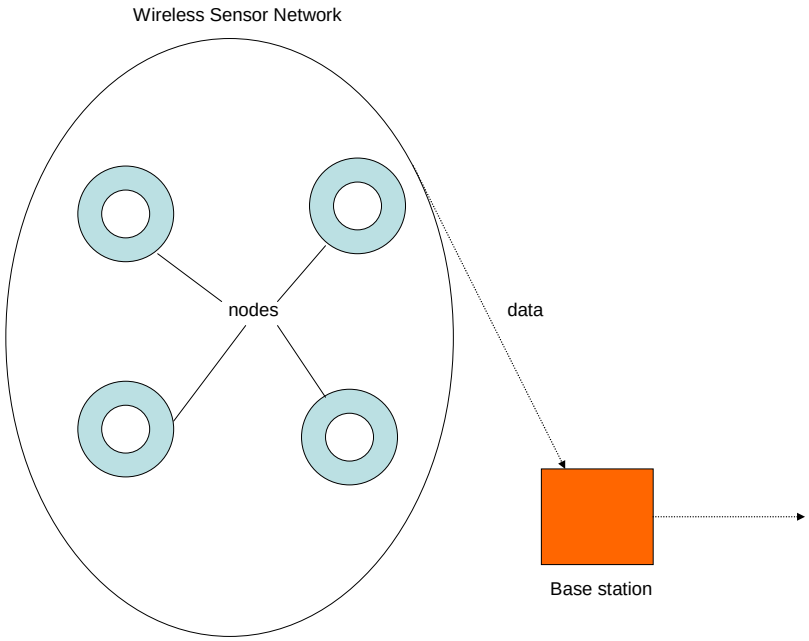

Figure 11. WSN data flow example

B. CROSSBOW MSP410

Many companies such as Crossbow, Ember, and Texas Instruments produce wireless sensor network components and solutions. Crossbow is a company specializing in inertial systems and wireless sensor network solutions. This thesis uses the Crossbow MSP410 wireless security system for implementing a WSN solution. The MSP410 package employs sensors used in various wireless intrusion detection systems and deploys as part of a robust mesh network of multi-purpose mote protection modules.

The MSP410 system consists of battery-powered motes housing a 433 MHz processor with magnetic, passive infrared, and acoustic detection capability. The system also uses a base station module to allow the sensor network data onto a personal computer.

Figure 12. Crossbow MSP410 mote (From xbow.com, September 2008)

Figure 13. Inner processor and detectors of MSP410 mote (From xbow.com, September 2008)

Figure 14. MSP410 Base Station (From xbow.com, September 2008)

The mesh-networking feature of the motes allows motes to communicate with each mote in the network. Additional motes can be added to the network or motes can be removed from the network seamlessly. The magnetic detection capability within the motes uses a two-axis magnetic field sensor to detect electronic voltage perturbations around the sensor. The passive infrared sensors detect dynamic changes in the thermal

radiation environment within immediate vicinity of the sensor. The mote also contains a dormant microphone to detect acoustic changes within its environment. Each mote contains four magnetic and passive infrared sensors placed within a cubicle housing to provide nearly 360-degree coverage.

Specifications	MSP410CA	Remarks
Processor Performance		
Program Flash Memory	128K bytes	
Measurement (Serial) Flash	512K bytes	> 100,000 Measurements
Configuration EEPROM	4K bytes	
Serial Communications	UART	0-3V transmission levels
Analog to Digital Converter	10 bit ADC	8 channel, 0-3Vin
Multi-Channel Radio		
Center Frequency	433 MHz	ISM bands
Number of Channels	4	programmable
Data Rate	38.4 Kbaud	manchester encoded
RF Power	-20 to +10 dBm	programmable, typical
Receive Sensitivity	-101 dBm	typical, analog RSSI at AD Ch. 0
Outdoor Range	> 250 ft	1/2 wave monopole, ground-level, LOS
	> 500 ft	1/2 wave monopole, elevated, LOS
Dual-Axis Magnetometer		
Range	± 6 gauss	
Sensitivity	1mV/V/Gauss	
Resolution	120 µGauss	at 50 Hz BW
Detection Range[1]	> 25 ft	
Passive Infrared Detectors		
Range	360°	10° increments
Optical Wavelength	5µm-14µm	
Bandwidth	0.01-15 Hz	optimal range
Look Angle	± 15°	
Detection Range[2]	> 25 ft	
Electromechanical		
Battery	2 x AA batteries	
Size (in)	3.56 x 3.63 x 2.38	excl. adjustable antenna
(mm)	77 x 77 x 51	excl. adjustable antenna
Weight (oz)	9	incl. batteries
(grams)	255	incl. batteries
Expansion Connector	51-pin	
Environmental		
Temperature	0 - 70° C	operating range
Package		weather resistant

Table 2. MSP410 Specifications (From xbow.com, September 2008)

C. WSN AS AN IED COUNTERMEASURE

Wireless sensor networking is an emerging technology rapidly incorporating itself into real world applications. The use of inconspicuous motes detecting physical properties information make it a natural fit for analyzing an IED urban scenario. WSN motes can be configured to detect numerous properties necessary for its usage purpose. Placing a WSN by entry and exit points of urban buildings provides a stealthy means of detecting IED materials. The accuracy of the mote detectors allows observers to distinguish normal routines from suspicious IED activities. The WSN can be setup to alert security officials of possible IED activity and used in conjunction with standard surveillance methods to provide a more complete and accurate depiction of actual activities taking place in real-time.

IV. WIRELESS SENSOR NETWORK CONFIGURATIONS AND EXPERIMENTS

A. FOCUS OF RESEARCH

The focus of this research is to find patterns of activity that lead to the discovery of IEDs by terrorists in urban environments. Urban settings include places of worship, shopping malls, offices, etc. The experiments concentrate upon detection of personal-borne IEDs (PBIEDs).

This research concentrates on employing a wireless sensor network (WSN) to provide a low power, easily deployable, and adaptable solution to detect IEDs. These characteristics of WSNs make it a possible solution in combating the IED problem. The network will work in a predictive mode by looking for patterns of activity that appear suspicious and raising alerts when a certain level of confidence has been achieved in the prediction.

Using wireless sensor motes to form a WSN, this research experiments with different mote configurations and various tests to discover new methods of detecting IEDs. There are many different types of sensing modalities used to detect suspicious IED behavior including passive infrared (PIR), magnetic, acoustic, seismic and chemical.

This project concentrates on detecting magnetic signature patterns to predict IED presence in an urban environment. Ferrous materials compose a large number of IEDs, making magnetic sensors a logical choice for detecting IEDs. However, magnetic sensors alone may not be sufficient in confirming IED presence. Two different possibilities exist in this experiment. The network may be susceptible to false positives (the network falsely detecting IEDs) or false negatives (failure of network to detect IED). Using a combination of different sensor modalities could mitigate false positives or false negatives. Although this project only concentrated on magnetic signatures, other sensor modalities could provide the basis for future research.

The urban environment presents many challenges in this research. Large crowds provide many variables unbeknownst to the planning process. For example, the presence of a metal shopping cart in a grocery store is a common occurrence, thus another reason to use metallic sensors in conjunction with other detection characteristics. Another issue is the emplacement of the wireless sensor nodes. Although relatively small, they must be carefully placed to avoid accidental detection. The experiments conducted in this project show characteristics and results of using the wireless sensor motes with magnetic detection capability.

B. RESEARCH METHODOLOGY

The research consisted of several rounds of experiments using the Crossbow MSP410 wireless motes. These motes possess passive infrared and magnetic detection capabilities. All of the experiments made use of the MSP410 motes, 18" orange safety cones to elevate the motes from the ground, and steel buckets and staples to simulate metallic IED material. The experiments are clustered into three types: configuration, initial, and optimal.

1. Configuration Experiments

The configuration experiments were designed to test the physical attributes, capabilities, and limitations of the Crossbow MSP410 motes. The tests were created only to find characteristics of the magnetic sensors within the motes.

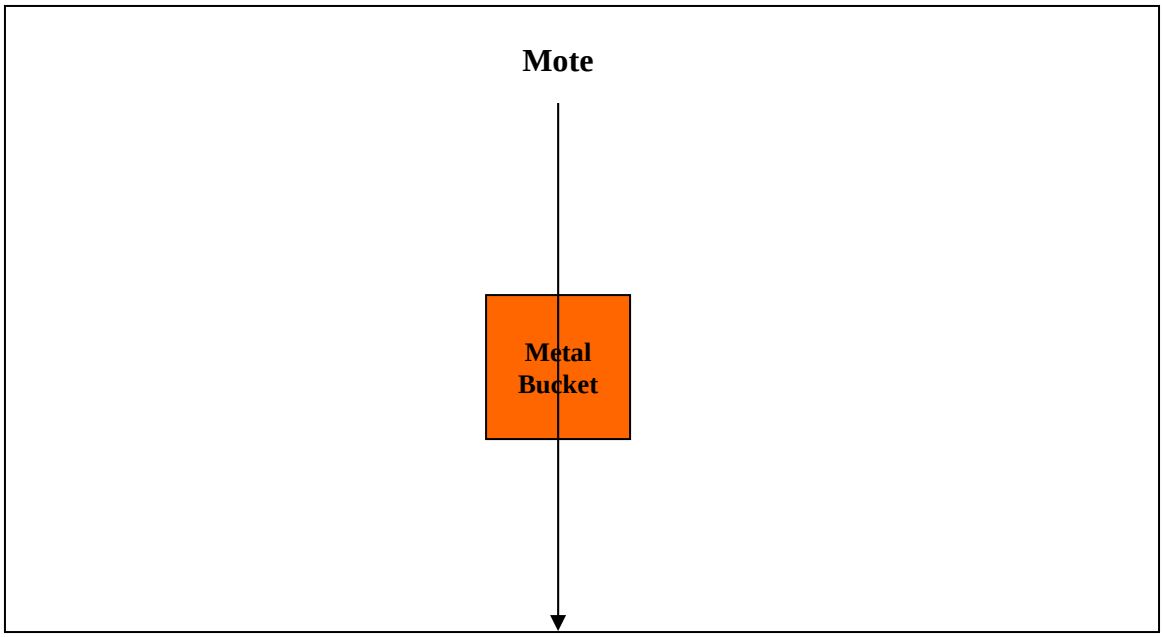

Figure 15. Configuration Experiment 1: Basic Setup

Configuration experiment 1 kept the metal bucket in a fixed position and the mote was walked along a straight-line path over the bucket. It was determined that the spacing was too great and the motes had trouble detecting magnetic material unless extremely close to the mote.

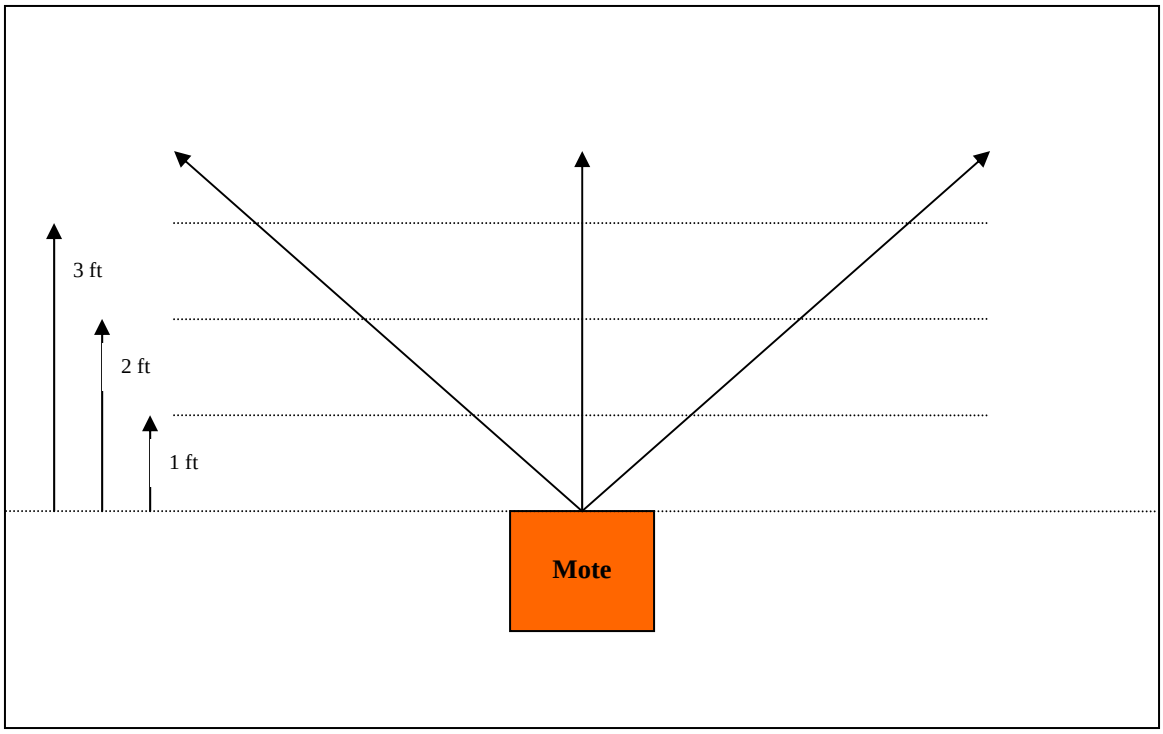

Figure 16. Configuration Experiment 2: Horizontal Cone angle configuration setup

Configuration experiment 2 tested for the cone angle of the mote. Finding the cone angle helped determine the optimal configuration of mote placements in a wireless sensor network. It was discovered that the mote had an 89-degree cone angle, giving the mote just under full 360-degree coverage.

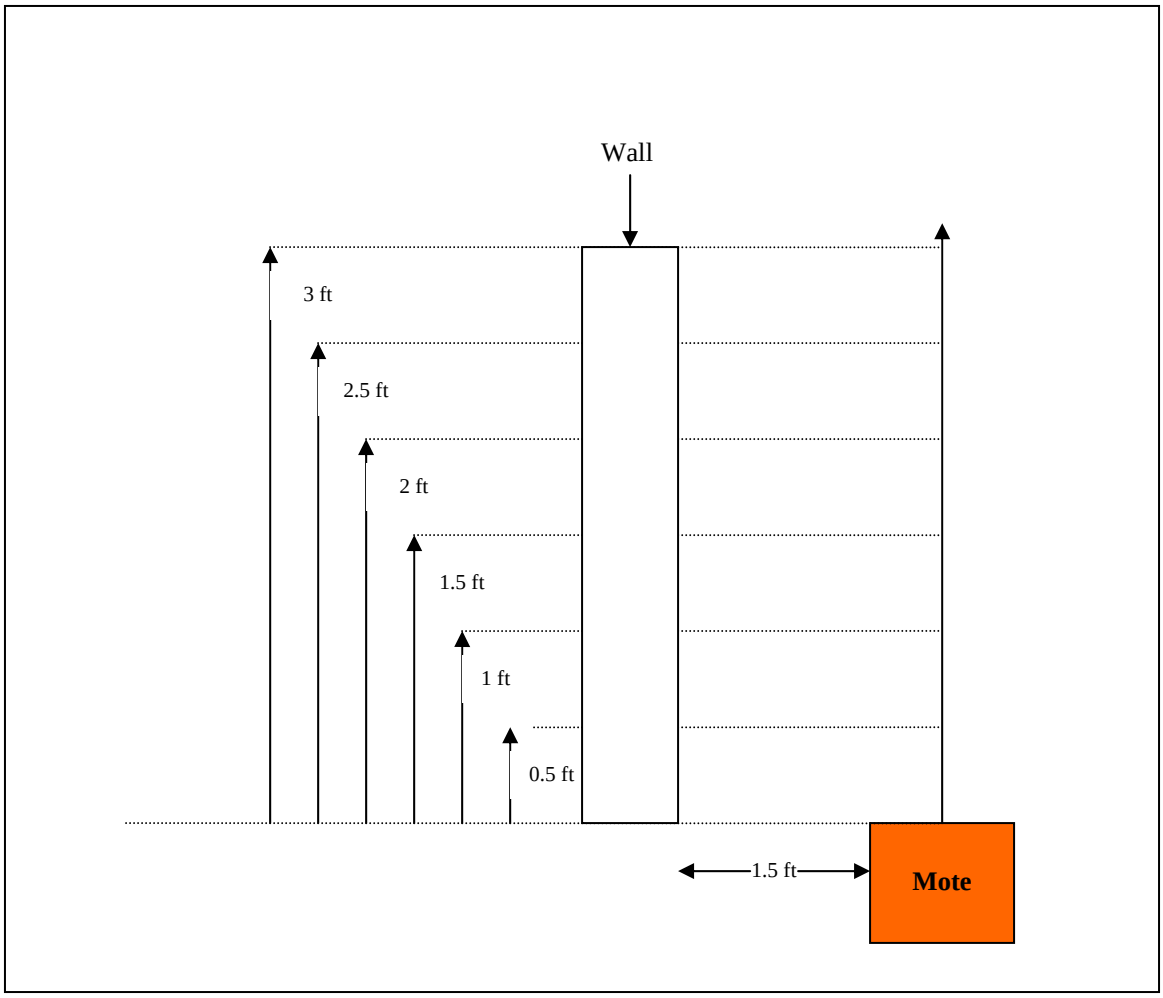

Figure 17. Configuration Experiment 3: Vertical Cone angle configuration setup

Configuration experiment 3 placed the mote 1.5 feet away from a wall. Metal was placed at varying heights of the wall to determine how high the metal could be detected by the sensor mote. Results showed that a 2.5' height was the maximum distance that still provided consistent results.

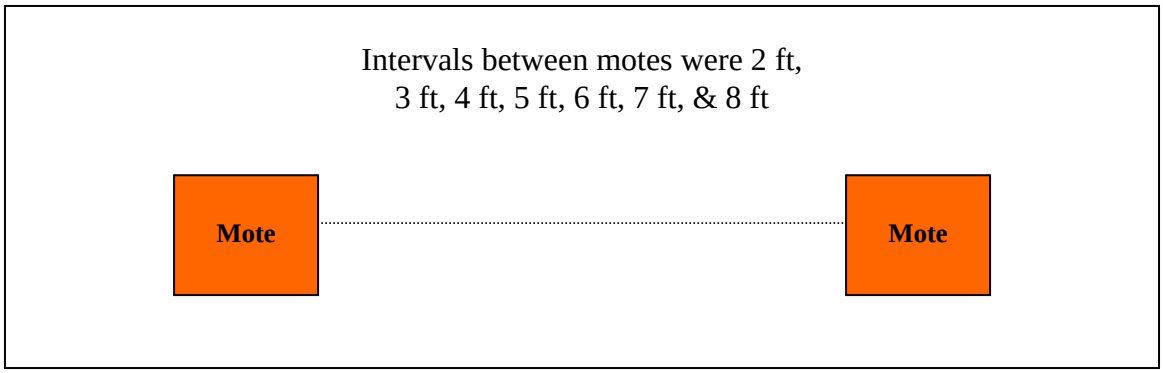

Figure 18. Configuration Experiment 4: Mote interval spacing setup

The capability of mote magnetic detection capability as a function of distance was needed. Configuration experiment 4 placed two motes at varying intervals to determine the maximum spacing between the motes that still allowed for detection of magnetic material. This experiment showed that six feet spacing produced reliable and consistent results. Later rounds of experiments show that eight feet spacing is acceptable for detection and still yields consistent results. This means that metal detection is strong when material is placed no more than four feet from the mote.

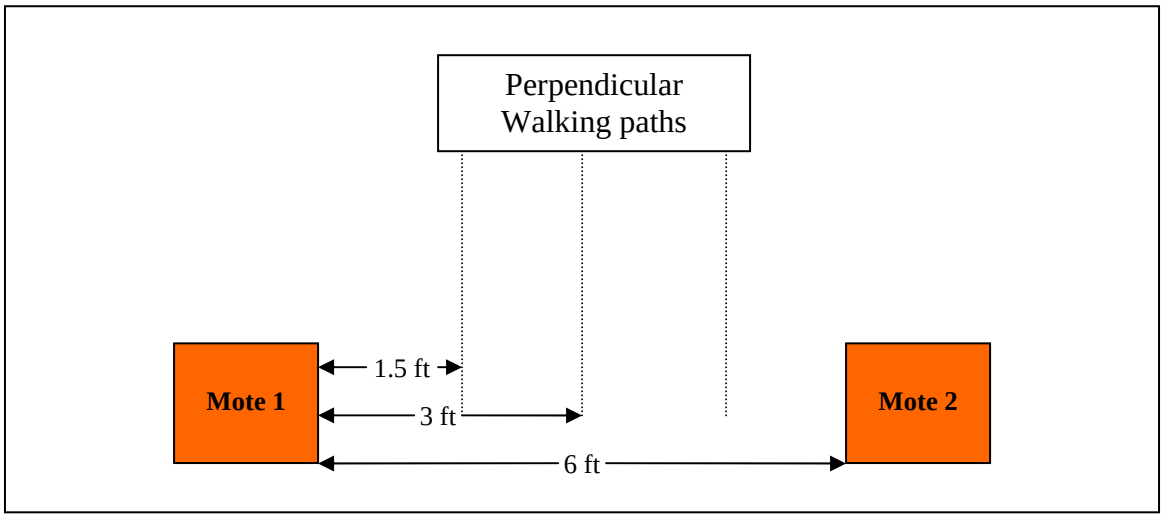

Figure 19. Configuration Experiment 5: Mote 1 distance vs. strength of reading

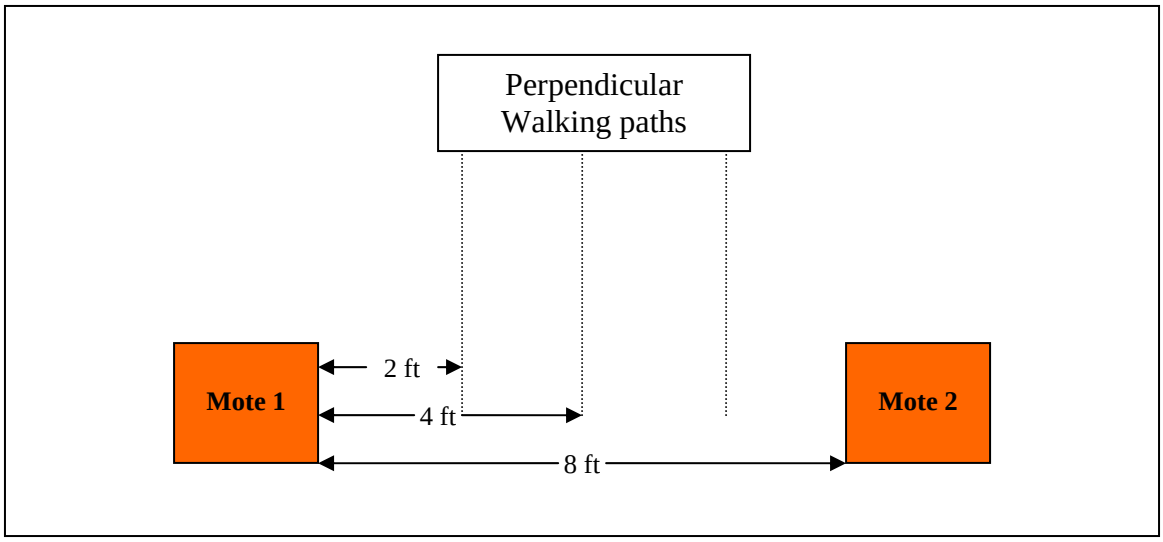

Figure 20. Configuration Experiment 6: Mote 2 distance vs. strength of reading

Configurations 5 and 6 tested whether the distance from the mote affected the strength of the magnetic readings. It was determined that the motes did produce stronger magnetic readings at closer distances. However, the mote's magnetic reading quickly saturated inside of 1.5 feet. This saturation made distance from the indeterminate at close distances.

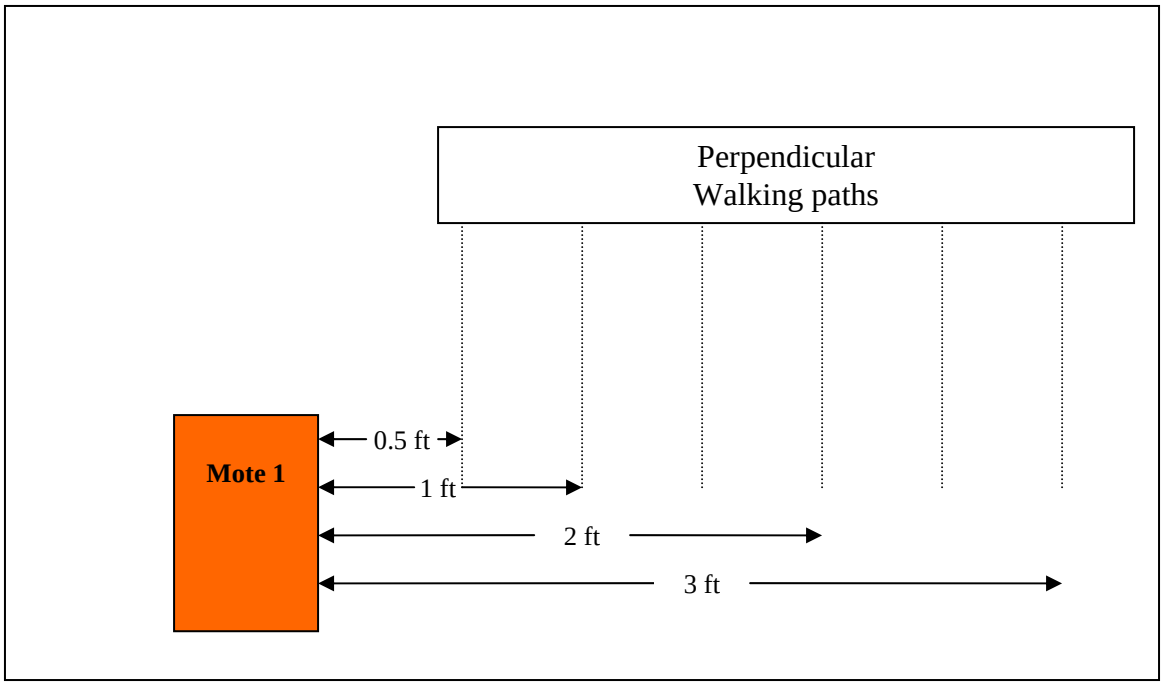

Figure 21. Configuration Experiment 7: Metal volume vs. strength of reading

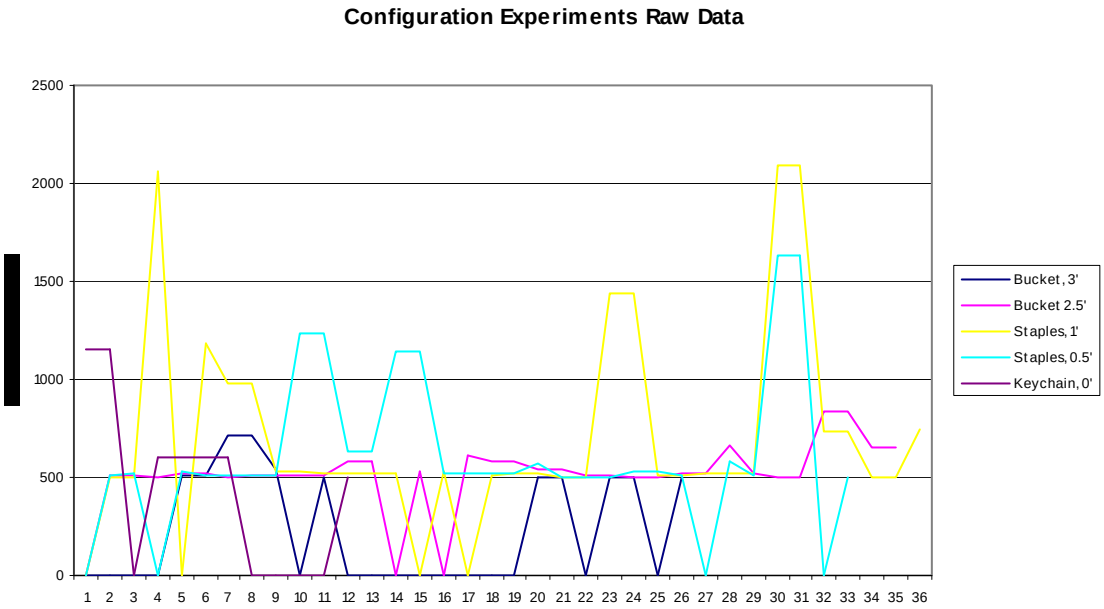

Figure 22. Raw data graph of metal amount vs. strength of reading

Configuration experiment 7 was a tested if large amounts of metal at a specified distance would give the same magnetic reading as smaller amounts of metal at a closer distance. It was found to be true. The graph shows various metals placed at various distances from the mote. A keychain placed 6 inches from the mote gave just as strong readings as a bucket placed 3 feet away from the mote.

2. Initial Setup Experiments

The initial setup experiments tested various configurations of a six mote wireless sensor network. These initial experiments combined with the configuration experiments lead to designing an optimal configuration of six motes.

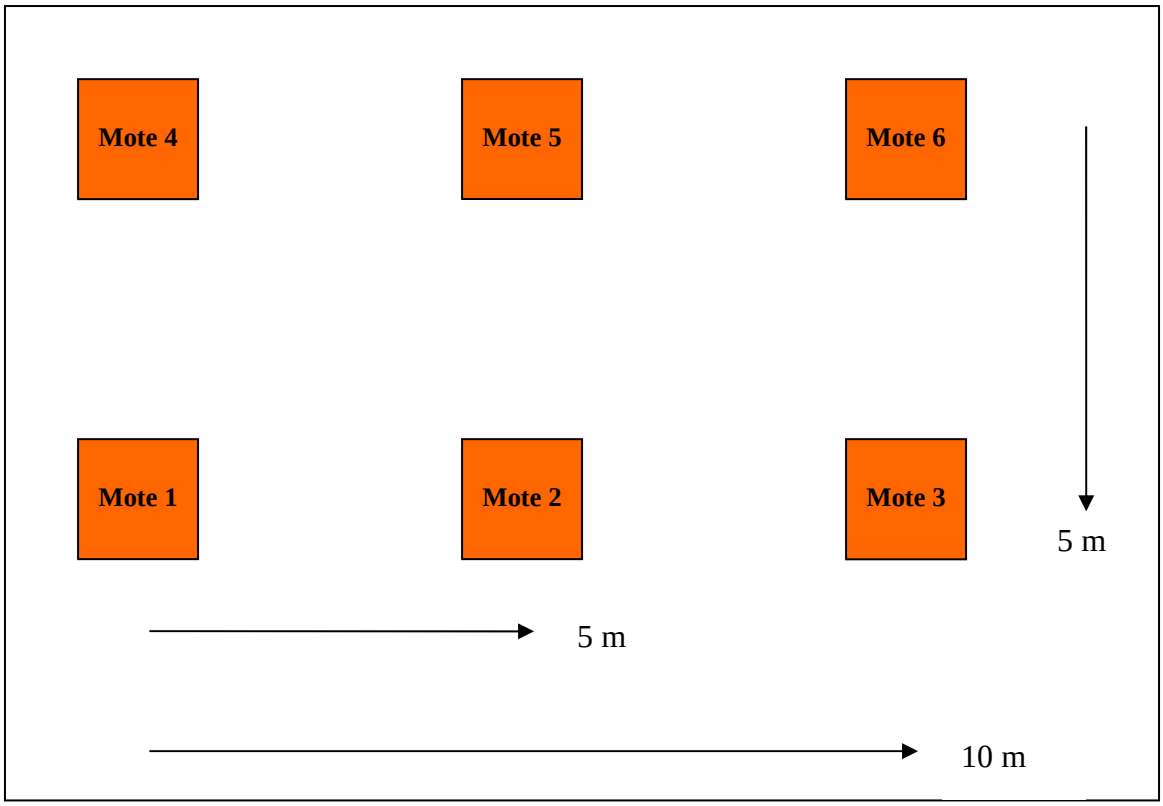

Figure 23. Initial Experiment 1: six-mote configuration

The first experiment used a basic rectangular configuration of motes placed at five-meter intervals as shown. During this experiment, the steel bucket was traversed through various paths around the motes. These various paths often produced dead spots

in which ferrous material was unable to be detected. It was determined that the motes were spaced too far apart causing the many "dead" spots in the configuration. The experiment was tested several times with the same results.

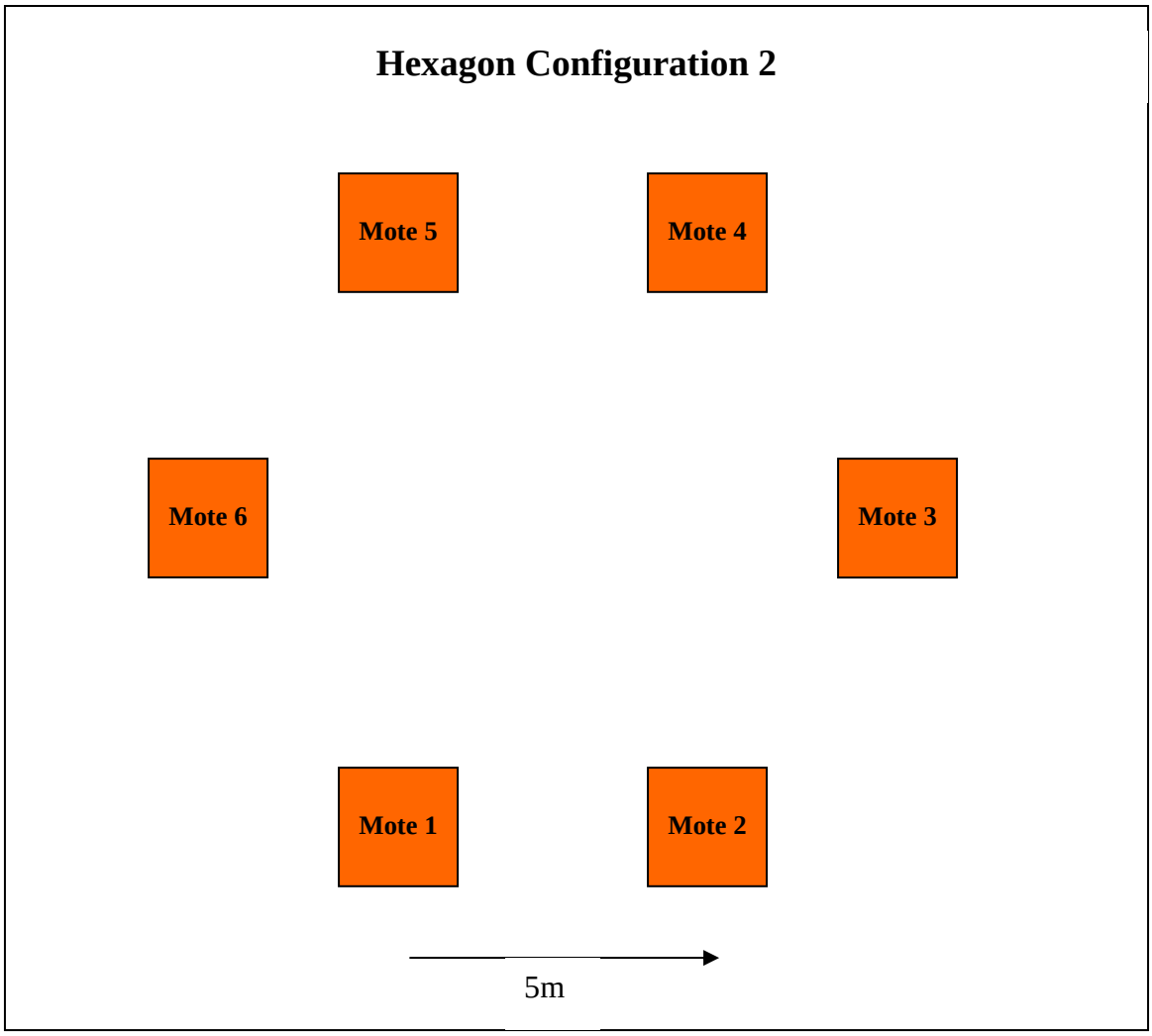

Figure 24. Initial Experiment 2: Hexagon six-mote configuration

Initial experiment 2 tested a hexagonal configuration of motes. Mote spacing was set at five-meter intervals again. The mote spacing was too great again. Although magnetic readings were strong near the motes, the strength of readings quickly decreased with increased distance from the motes. Various walking paths through the network were tested with similar results.

3. Optimal Configuration Experiments

Through the configuration and initial setup experiments, the following design was found to be optimal for a six-mote wireless sensor network. Motes one and five represent an entrance or doorway to an urban building. The first experiments using the optimal configuration placed the motes at two feet intervals. This interval was later increased to four feet, eight feet, and 12 feet. Initial experiments used one subject carrying a metal bucket to traverse the network. Final experiments were conducted with two and three subjects traversing the network with differing amounts of metal.

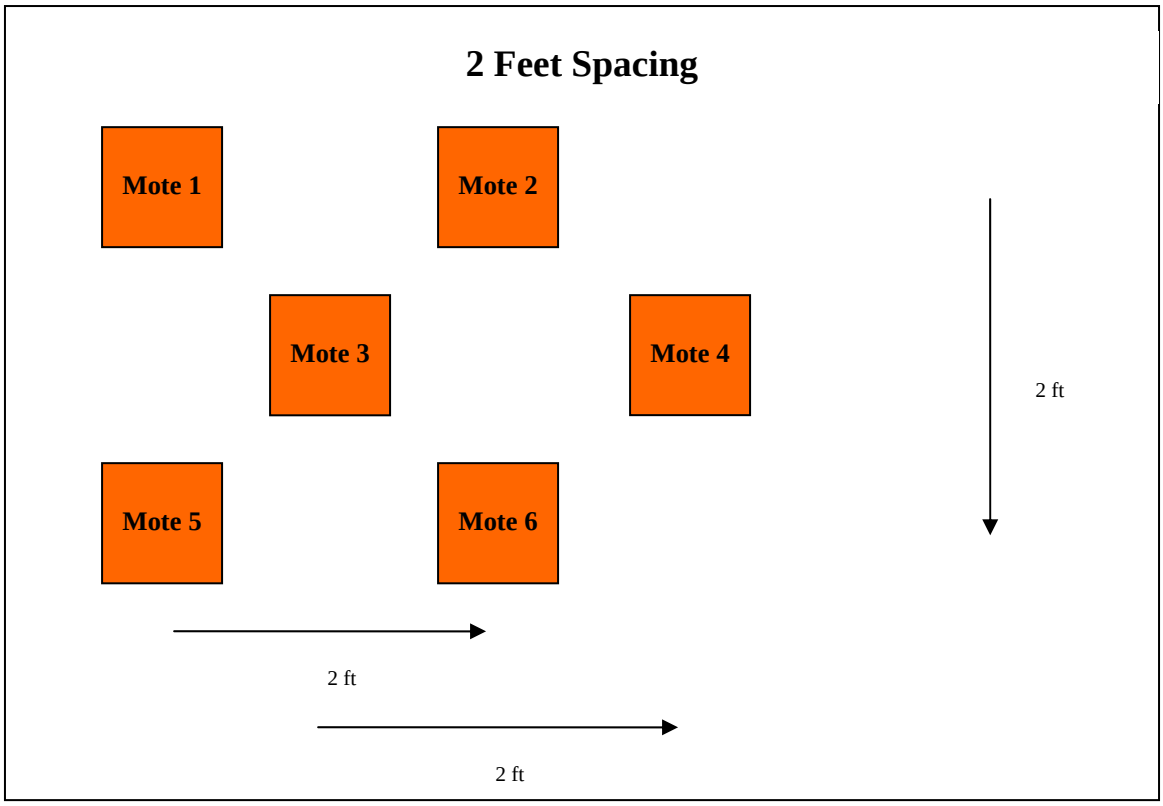

Figure 25. Optimal Experiment 3: Optimal six-mote configuration with two feet intervals

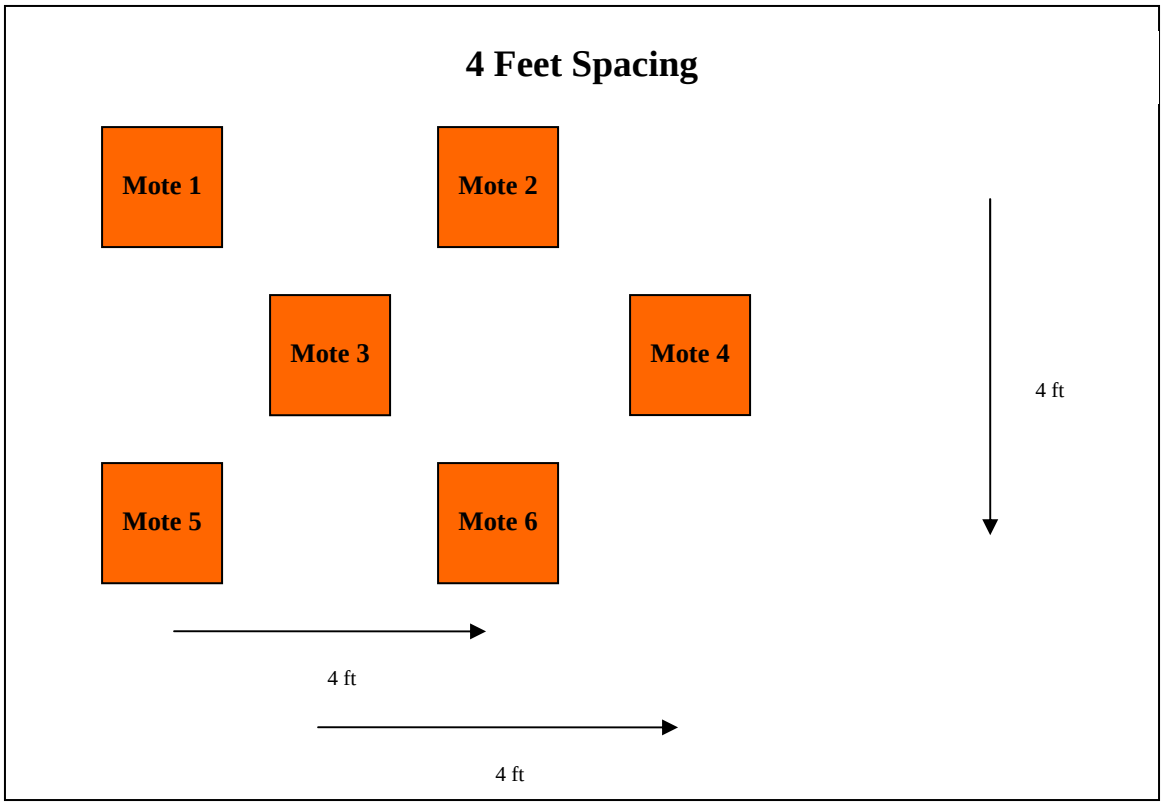

Figure 26. Optimal Experiment 4: Optimal six-mote configuration with four feet intervals

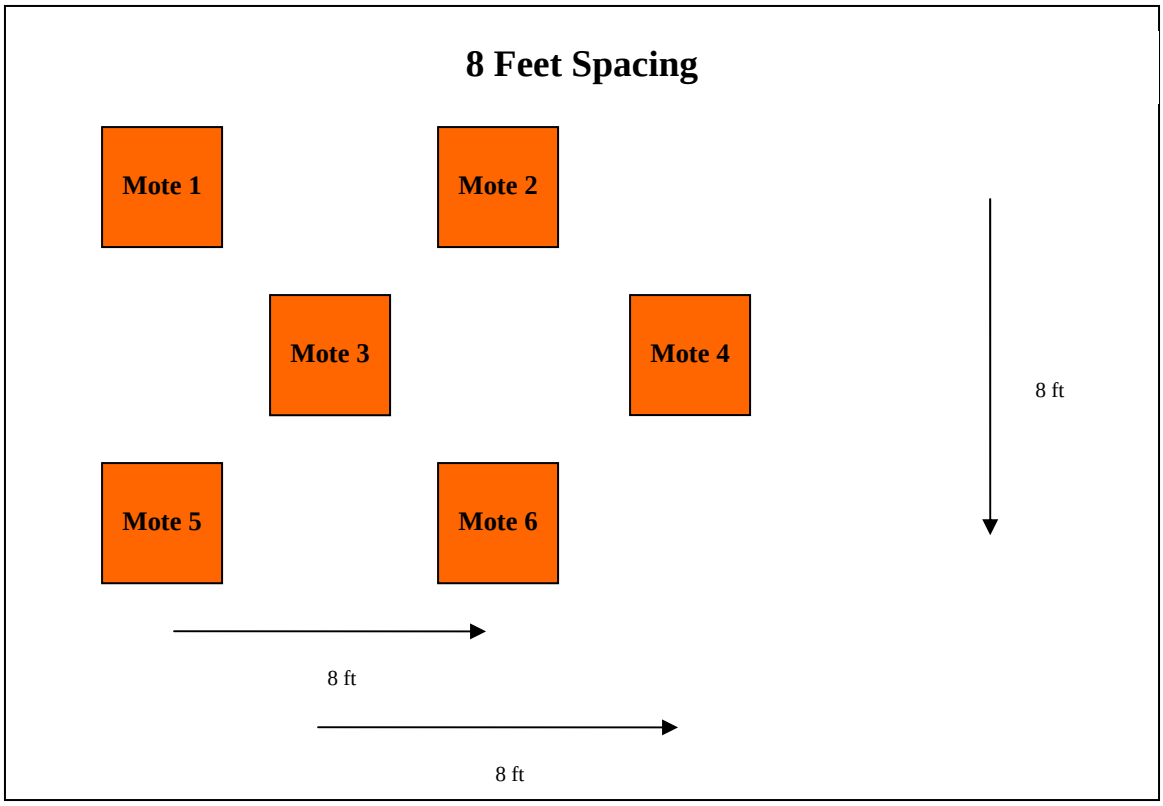

Figure 27. Optimal Experiment 5: Optimal six-mote configuration with eight feet intervals

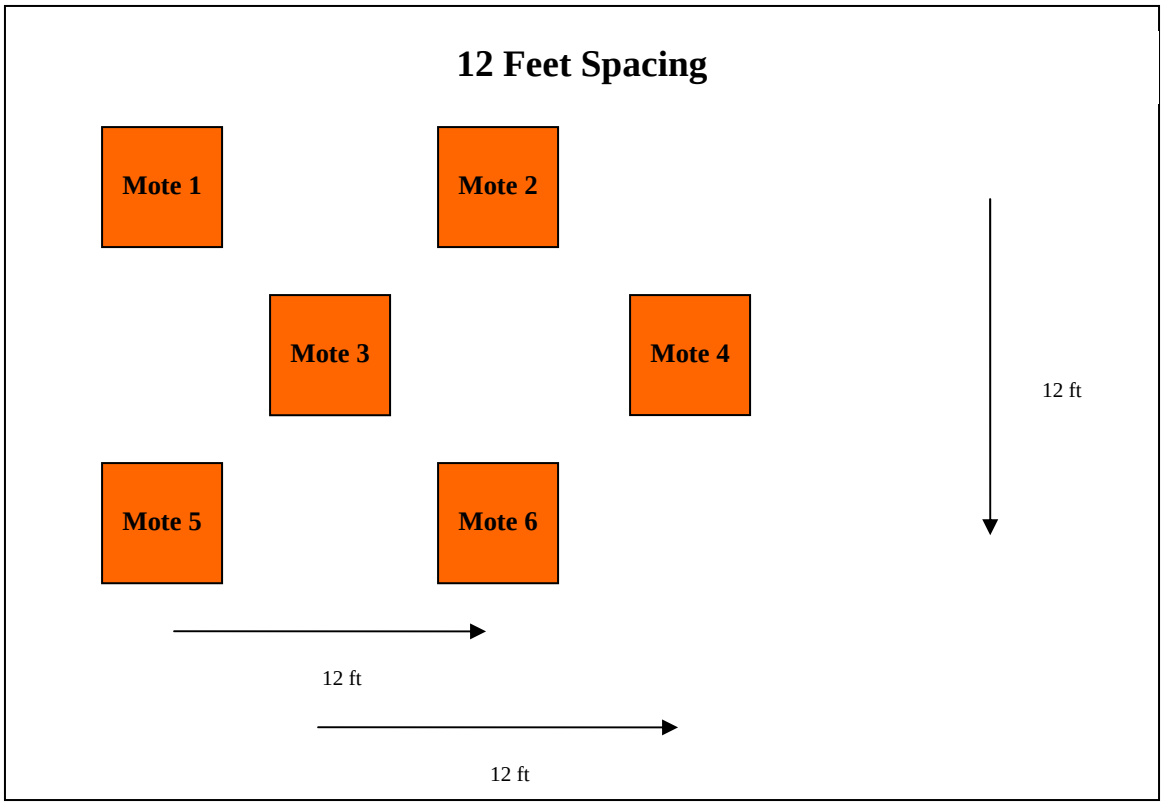

Figure 28. Optimal Experiment 6: Optimal six-mote configuration with 12 feet intervals

Initial experiments tested the two and four feet configurations as a means of providing network redundancy and avoiding blind spots inside the mote area. The motes were able to detect strong magnetic signals from the bucket and provided many data points for detection by the mote software. Saturation was a factor in these experiments.

Later experiments expanded the mote intervals to eight and twelve feet. The eight-foot configuration still provided reliable and consistent results. The twelve-foot configuration showed some readings, but was not consistently able to detect metal from six feet away. From several rounds of experiments, it was determined that an eight-foot interval between motes was optimal for the six-mote network. This interval provided redundancy of motes while avoiding blind spots within the network. However, this assumes that motes one and five provide the only entrance point into the network.

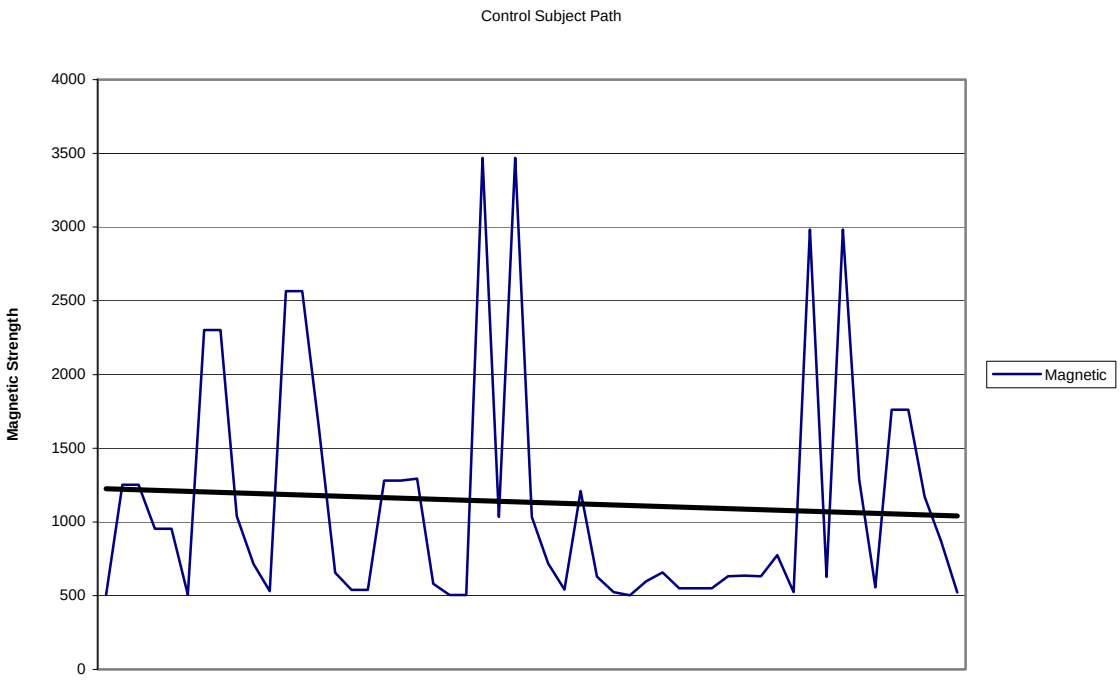

Figure 29. Control subject path in multi-person experiment

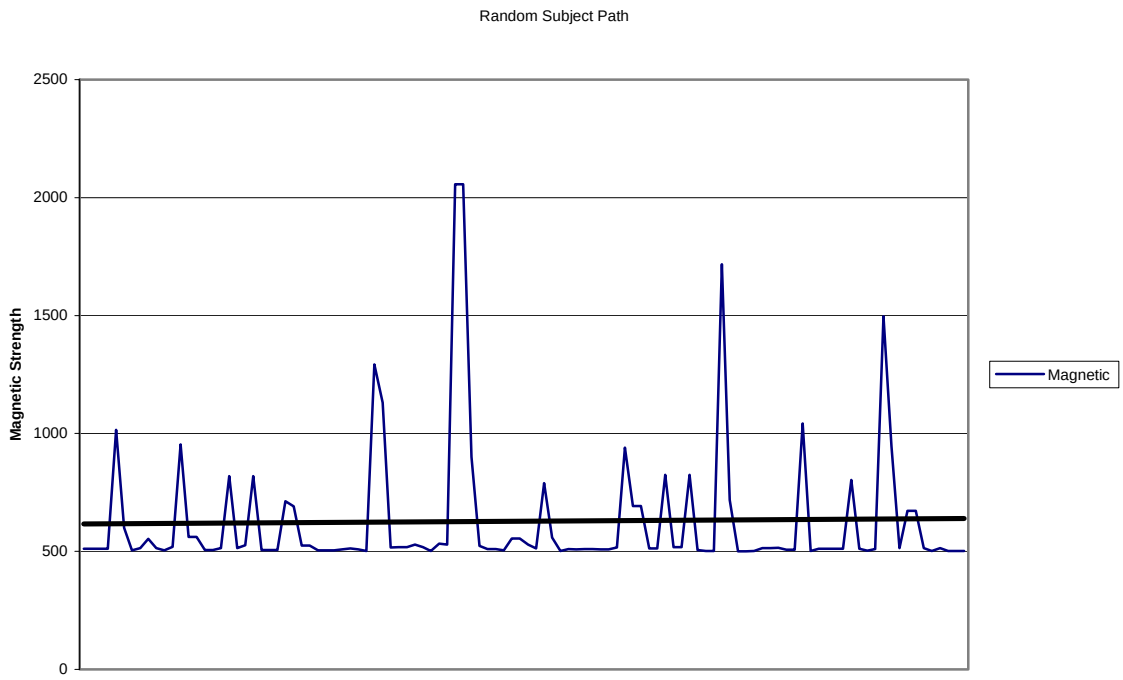

Figure 30. Random subjects path in multi-person experiment

Subsequent experiments increased the number of subjects traversing the network. The above graphs represent a singular experiment where one subject with a small amount of metal walked directly over motes one and two and another subject carrying a metal bucket walked a straight-line path between motes three, four, five, and six. Both subjects showed strong readings, further demonstrating the effects of distance versus amount of metal.

Final experiments used two or three subjects traveling the network. A control subject carried a steel bucket along a pre-ordained path, while other subjects carried nominal amounts of metal to represent normal conditions like carrying key chains and jewelry. Some experiments had the subjects walking in parallel. Other experiments had the subjects traversing the networks in opposite directions. Final experiments had subjects walking randomly through the network. The experiments showed consistent results in that the steel bucket was always detectable. Small amounts of metal were detected when subjects were in close proximity to the wireless mote. Another factor tested for was walking pace. Pace did not affect the strength of readings in the experiments.

V. CONCLUSIONS

A. OVERALL IMPRESSIONS

Overall, a wireless sensor network using only magnetic detection is not a complete and reliable solution for the IED problem. The strengths of a WSN include low power requirements, adaptability, and relative ease of use. Weaknesses include a lack of processing power, difficult software changes, and susceptibility to jamming.

The MSP410 wireless motes were severely limited in their magnetic detection capability. The motes work well when detecting large amounts of metals (i.e. cars) or metal at close distance (less than 12”). At distances of less then 12”, the motes accurately detect small amounts of metal such as a cell phone or keychain, but this ability quickly tapers off outside of 18”. The motes could reliably detect the five-gallon steel bucket weighing three pounds from 4 feet. Distances greater then 4 feet did not provide reliable and consistent detection capability. The inability of the motes to detect at greater distances makes the MSP410 equipment an expensive solution for urban environments. For controlling entrances to building such as shopping malls, places of worship or office buildings, a cost-effective WSN implementation would be possible. It will require designing and integrating a configuration that leaves no holes in detection and provides redundancy to prevent network failure.

The wireless sensor network is extremely vulnerable to electromagnetic jamming. An attack could take place by first using a spectrum analyzer to determine the frequency of the mote communication. A signal generator could then re-create the signal at the same frequency but at a higher power setting to jam the network. One possible solution is to employ frequency hopping. The SP410 motes do not support frequency hopping in their firmware.

B. FUTURE WORK SUGGESTIONS

There are many suggestions for future work in this project. First, the motes need to be able to sample at a higher rate to more accurately show readings compared to distance from the mote. This might be achieved through a software fix or new wireless sensor mote equipment. It is often impossible to tell whether a reading is a small amount of metal at close distance, or a larger amount of metal at an increased distance from the mote. Other sensor capabilities can be tested with the motes. Through infrared sensing, motes can measure magnetic readings in conjunction with infrared signatures. This is one possible solution in distinguishing varying amounts of metal with respect to mote distance.

Although many tests have been completed in the research reported here, more research and experimentation is needed. The sensor network would be extremely successful in an urban environment if given a constant power source and an increased magnetic sampling rate. In addition, activating additional sensor modalities should be tested to see if they could be used in conjunction with magnetic sensing to provide better results. This would allow for a better depiction of patterns consistent with IED emplacement. Through further testing, the sensor network can truly utilize its full potential as a solution for IED detection.

LIST OF REFERENCES

Atkinson, Rick. "If you don't go after the network, you're never going to stop these guys. Never." *The Washington Post* 03 October 2007. Retrieved September 2008, from <http://www.washingtonpost.com/wp-dyn/content/article/2007/10/02/AR2007100202366.html>

Atkinson, Rick. "The IED problem is getting out of control. We've got to stop the bleeding." *The Washington Post* 30 September 2007. Retrieved September 2008, from <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/29/AR2007092900751.html>

Atkinson, Rick. "The single most effective weapon against our deployed forces." *The Washington Post* 30 September 2007. Retrieved September 2008, from <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/29/AR2007092900750.html>

Atkinson, Rick. "There was a two-year learning curve . .and a lot of people died in those two years." *The Washington Post* 01 October 2007. Retrieved September 2008, from <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/30/AR2007093001675.html>

Atkinson, Rick. "You can't armor your way out of this problem." *The Washington Post* 02 October 2007. Retrieved September 2008, from <http://www.washingtonpost.com/wp-dyn/content/article/2007/10/01/AR2007100101760.html>

Bourzac, Katherine. "Tiny, Sensitive Magnetic-Field Detectors: Arrays of cheap magnetic sensors could detect improvised explosive devices." *Technology Review*, Massachusetts Institute of Technology 16 November 2007. Retrieved September 2008, from <http://www.technologyreview.com/Biotech/19724/>

Chisolm, Patrick. "Clearing the Roads." Special *Operations Technology Online Editio*n. 2 July 2008. Retrieved September 2008, from <http://www.special-operations-technology.com/article.cfm?DocID=1129>

Clark, Roger. "About Imaging Spectroscopy." U.S. Geological Survey 25 September 2002. Retrieved September 2008, from <http://speclab.cr.usgs.gov/aboutimsp.html>

Collins, Michael. "Wireless Sensor Network Helps Grower Produce Better Grapes." *BBC News Online* 6 July 2004. Retrieved September 2008, from <http://news.bbc.co.uk/2/hi/technology/3860863.stm>

Farr, Keith. "ULTOR: Ultra Lethal Targeting by Optical Recognition." Advanced Optical Systems, Inc. 2006. Retrieved September 2008, from <http://www.aos-inc.com/research/TechBriefPDFs/ULTORTechBrief.pdf >

Hall, Mimi. "Feds focus on detecting bombs." *USA Today* 27 November 2007. Retrieved September 2008, from <http://www.usatoday.com/news/nation/2007-11-26-bomb-detection_N.htm>

Hendrickx et al. "New Mexico Tech Landmine, UXO, IED Detection Sensor Test Facility: Measurement in Real Field Soils." New Mexico Institute of Mining and Technology 27 April 2006.

Huffman, Ethan. "INL's Explosive Detection System to be installed at US Air Base." Idaho National Laboratory 21 November 2006. Retrieved September 2008, from <http://www.inl.gov/featurestories/2006-11-21.shtml>

icasualties.org Iraq Coalition Casualty Count. July 2008. Retrieved September 2008, from <http://icasualties.org/oif/IED.aspx>

JIEDDO: Joint IED Defeat Organization. Retrieved September 2008, from <https://www.jieddo.dod.mil>

Mainwaring et al. "Wireless Sensor Networks for Habitat Monitoring." *WSNA '02*, Atlanta, GA 28 September 2002.

Saletan, William. "The Jihadsons: Technology Lessons from the Iraq War." *Slate Magazine* 12 October 2007. Retrieved September 2008, from <http://www.slate.com/id/2175723/>

Tissue, Brian. "Raman Spectroscopy." Science Hypermedia Home Page 24 February 1996. Retrieved September 2008, from <http://elchem.kaist.ac.kr/vt/chem-ed/spec/vib/raman.htm>

Wilson, Clay. "Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures." CRS Report for Congress 28 August 2007.

Zhao, Feng and Guibas, Leonidas. *Wireless Sensor Network: An Information Processing Approach.* Morgan Kaufmann Publishers, San Francisco, CA 2004.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California